| Notice of Allowability | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/740,457 | CHEN ET AL. | |
| | Examiner | Art Unit | |
| | Zachary A Davis | 2137 | |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--***

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *The Amendment after Final Rejection received 17 March 2005*.

2. ☒ The allowed claim(s) is/are *1-3,5 and 6*.

3. ☒ The drawings filed on *30 July 2001* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   **Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Andrew Caldwell

**ANDREW CALDWELL**
**SUPERVISORY PATENT EXAMINER**



TE

## DETAILED ACTION

1. An amendment was received after Final rejection on 17 March 2005. Claims 3 and 5 have been amended. Claim 4 has been canceled. No new claims have been added. Claims 1-3, 5, and 6 are pending in the present application.

### *Allowable Subject Matter*

2. Claims 1-3, 5, and 6 are allowed.

3. The following is an examiner's statement of reasons for allowance:

Independent Claims 1 and 2 are directed to a method and apparatus for determining A mod N using a calculating engine based on the Montgomery multiplication algorithm. The closest prior art, Tenca and Koc, "A Scalable Architecture for Montgomery Multiplication", hereinafter "Tenca", also discloses a method for determining the modular reduction of A mod N; however, Applicant argues that Tenca does not teach or suggest that both inputs of the Montgomery multiplication engine are processed word by word, and instead teaches that at least one of the inputs is processed bit by bit. This argument is persuasive, and the claims are therefore allowable.

Independent Claims 3 and 6 are directed to a method and apparatus for determining $A^B$ mod N using a calculation engine based on the Montgomery multiplication algorithm and using operations implementing the Chinese Remainder

Theorem. The closest prior art, Tenca in view of Compaq Computer Corporation, "Cryptography Using Compaq MultiPrime Technology in a Parallel Processing Environment", hereinafter "Compaq", also discloses a method for determining the modular exponentiation $A^B$ mod N; however, Applicant similarly argues that, for the reasons above, neither Tenca nor Compaq teach or suggest, alone or in combination, that both inputs of the Montgomery multiplication engine are processed word by word, and that Tenca instead teaches that at least one of the inputs is processed bit by bit. This argument is persuasive, and the claims are therefore allowable.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

zad

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER